**Аспекты ИБ**

На практике важнейшими являются три аспекта информационной безопасности  
(модель КЦД, или CIA):

**Конфиденциальность (confidentiality)** — гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена. Нарушение этой категории называется хищением либо раскрытием информации.

**Целостность (integrity)**— гарантия того, что информация сейчас существует в её исходном виде, то есть при её хранении или передаче не было произведено несанкционированных изменений. Нарушение этой категории называется фальсификацией сообщения.

**Доступность (availability)**— гарантия того, что требуемую информационную услугу можно получить за разумное время.

Помимо этого часто выделяют ещё 2 категории ИБ, которые, в общем случае, можно отнести к категории **«целостность»:**

1. **Аутентичность (подлинность)** — гарантия того, что источником информации является именно то лицо, которое заявлено как её автор. Нарушение этой категории называется фальсификацией автора сообщения.
2. **Апеллируемость (неотказуемость)**— гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой. В отличие от аутентичности, где при подмене автора, кто-то другой пытается заявить, что он автор сообщения, при нарушении апеллируемости сам автор пытается отказаться от своих слов, подписанных им однажды.

Свойство **конфиденциальности**, примененное к устройству печати, можно интерпретировать так, что доступ к устройству имеют те и только те пользователи, которым этот доступ разрешен, причем они могут выполнять только те операции с устройством, которые для них определены.

Свойство **доступности**устройства означает его готовность к использованию всякий раз, когда в этом возникает необходимость.

А свойство **целостности**может быть определено как свойство неизменности параметров настройки данного устройства. Легальность использования сетевых устройств важна не только постольку, поскольку она влияет на безопасность данных. Устройства могут предоставлять различные услуги: распечатку текстов, отправку факсов, доступ в Интернет, электронную почту и т. п., незаконное потребление которых, наносящее материальный ущерб предприятию, также является нарушением безопасности системы.

**Защита информации**— комплекс мер по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Понятия КЦД могут быть определены не только по отношению к информации, но и к другим программным и аппаратным ресурсам, например внешним устройствам или приложениям. Существует множество системных ресурсов, возможность «незаконного» использования которых может привести к нарушению безопасности системы. Например, неограниченный доступ к устройству печати позволяет злоумышленнику получать копии распечатываемых документов, изменять параметры настройки, что может привести к изменению очередности работ и даже к выводу устройства из строя.

Системы информационной безопасности должны уметь противостоять разнообразным атакам: как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды, иногда прощупывание уязвимых мест ведётся медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ: доступности, целостности или конфиденциальности.

**Характеристики безопасной ИС**

**Безопасная ИС**— это система, которая, во-первых, защищает данные от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, а в-третьих, надёжно хранит информацию и гарантирует неизменность данных. Таким образом, безопасная ИС по определению обладает свойствами КЦД.

**Конфиденциальность**— самый проработанный у нас в стране аспект информационной безопасности. Однако информационные системы создаются (приобретаются) для получения определённых информационных услуг. Поэтому, не противопоставляя доступность остальным аспектам, зачастую её можно считать важнейшим элемент ИБ. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления: в производстве, на транспорте. Весьма неприятные последствия может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т. п.).

**Целостность**оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, набор и характеристики комплектующих изделий, ход технологического процесса — всё это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница веб-сервера какого-либо государственного учреждения.

Анализ интересов различных категорий субъектов информационных отношений показывает, что почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность: какой смысл в информационной услуге, если она содержит искажённые сведения? Наконец, конфиденциальные моменты есть также у многих организаций (в тех же учебных заведениях недопустимо разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

Для того чтобы ИС обеспечивала свойства КЦД, необходимо, чтобы она обладала рядом характеристик:

1. **Надёжность**— гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано.
2. **Точность**— гарантия точного и полного выполнения всех команд.
3. **Контроль доступа**— гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются.
4. **Контролируемость**— гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса.
5. **Контроль идентификации** — гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает.
6. **Устойчивость к умышленным сбоям** — гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как предусмотрено заранее.

**Ситуация: нарушения аспектов ИБ**

«Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (Government Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники».

«Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, AP, 17 сентября 1996 года)».

«В середине июля 1996 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару».

«В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом».

«Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что её соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии».

«Ученые из Калифорнийского университета в Беркли считают, что аудиозапись работы пользователя на клавиатуре можно расшифровать. Метод основан на том, что каждая клавиша при нажатии издает характерный только для неё звук, и пользователи, которые обычно набирают примерно 300 знаков в минуту, оставляют достаточно времени между ударами, чтобы компьютер мог выделить отдельные звуки. В процессе исследования несколько 10-минутных записей работы пользователей были обработаны на компьютере с применением алгоритма, который расшифровывает до 96 % вводимых символов».

«Просматривая спутниковые снимки Сеула на сайте Google Earth , южнокорейские военные обнаружили оборонные предприятия и воинские части, правительственный комплекс Чонг Ва-Да (Cheong Wa-Dae) и ряд других засекреченных объектов. Там же можно было увидеть офис президента, командный центр армии и военные базы по всей стране. По корейским законам об охране военной тайны, военные базы и главные правительственные здания относятся к категории «основные объекты национальной безопасности», и их фотографирование строго запрещено, сообщает Chosun».

«В середине июня 2004 года электронные ресурсы правительства Южной Кореи подверглись массированной хакерской атаке. Неизвестному удалось заразить вирусом более 64 компьютеров, в том числе сайт Министерства обороны Южной Кореи. О проведённой атаке сообщил Южнокорейский центр кибербезопасности (NCSC). По официальным данным, хакеру удалось инфицировать с помощью троянской программы Peep Trojan компьютеры Агентства по разработке средств защиты, которое занимается разработкой вооружений, Института по атомной энергии, а также вывести из строя несколько правительственных сайтов (в частности, порталы Морского министерства и Морской полиции Южной Кореи). После обнаружения атаки, специалисты NCSC приняли экстренные меры, блокировав сайт, на который вирусы должны были отослать конфиденциальную информацию. Саму утечку удалось предотвратить. Напомним, что южнокорейские власти не раз говорили о кибернетической угрозе со стороны Северной Кореи. Обучение хакеров там якобы поставлено на поток, и военная академия имени Ким Ир Сена ежегодно выпускает около сотни боевых хакеров».

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

*Интересы личности в информационной сфере* заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

*Интересы общества в информационной сфере* заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

*Интересы государства в информационной сфере* заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

**Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:**

**Первая составляющая национальных интересов Российской Федерации в информационной сфере** включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

* повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
* усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;
* обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
* обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
* укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
* гарантировать свободу массовой информации и запрет цензуры;
* не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
* обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

**Вторая составляющая национальных интересов Российской Федерации в информационной сфере** включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

* укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
* интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

**Третья составляющая национальных интересов Российской Федерации в информационной сфере** включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

* развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;
* развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
* развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
* обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

**Четвертая составляющая национальных интересов Российской Федерации в информационной сфере** включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

* повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
* интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
* обеспечить защиту сведений, составляющих государственную тайну;
* расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

**Основные положения государственной политики обеспечения информационной безопасности Российской Федерации**

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

* соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
* открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
* правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
* приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

* проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;
* организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;
* поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
* осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
* проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
* способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
* формулирует и реализует государственную информационную политику России;
* организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;
* способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации.

Это предполагает:

* оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;
* создание организационно-правовых механизмов обеспечения информационной безопасности;
* определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере;
* создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;
* разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;
* разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;
* совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

**Основные функции системы обеспечения информационной безопасности Российской Федерации**

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

* разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
* создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
* определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
* оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
* координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;
* контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;
* предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
* развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
* организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
* проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
* организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
* защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
* обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
* совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;
* осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

**Общие методы обеспечения информационной безопасности Российской Федерации**

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

* внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;
* законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
* разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
* уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
* законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
* определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
* создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.
* Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:
* создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
* усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
* разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
* создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
* выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
* сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
* совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
* контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
* формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

* разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
* совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.